UNDERSTANDING SOFTWARE ASSURANCE

Software: Computer programs, procedures, rules, and associated documentation and data pertaining to the development and operation of a computer system. Software includes programs and operational data contained in hardware (e.g., firmware, programmable logic, and programmable gate arrays). This also includes COTS, GOTS, MOTS, reuse, legacy, and heritage software products and components.

Software Quality: The discipline of software quality is a planned and systematic set of activities to ensure quality is built into the software. It consists of software quality assurance, software quality control, and software quality engineering. As an attribute, software quality is (1) the degree to which a system, component, or process meets specified requirements; or (2) the degree to which a system, component, or process meets customer or user needs or expectations.

Software Quality Assurance: The function of software quality that assures that the standards, processes, and procedures are appropriate for the project and are correctly implemented.

Software Quality Engineering: The function of software quality that assures that quality is built into the software by performing analyses, trade studies, and investigations on the requirements, design, code, and verification processes and results to assure that reliability, maintainability, and other quality factors are met.

Software Reliability: The discipline of software assurance that (1) defines the requirements for software controlled system fault/failure detection, isolation, and recovery; (2) reviews the software development processes and products for software error prevention and/or reduced functionality states; and (3) defines the process for measuring and analyzing defects and defines/derives the reliability and maintainability factors.

Software Safety: The discipline of software assurance that is a systematic approach to identifying, analyzing, tracking, mitigating, and controlling software hazards and hazardous functions (data and commands) to ensure safe operation within a system.

Independent Verification and Validation (IV&V): IV&V, as a part of software assurance, plays a role in the overall NASA software risk mitigation strategy applied throughout the life cycle, to improve the safety and quality of software.

☑ YOUR PREPAREDNESS FOR AN AUDIT OF NASA SOFTWARE ASSURANCE STANDARD WITH THESE SAMPLE AUDIT GUIDE QUESTIONS.

CENTER SMA MANAGEMENT:

1. What are the Center SA Procedures and processes in place that are scoped and tailored from the SA Standard to meet Center needs?
2. Verify that Software Assurance Classification Assessments are documented for every project.
3. What training is available for Software Assurance personnel? What training is completed?
4. Which projects are identified as having safety-critical software?
5. Is there an effective software change control program in place? Identify inclusion of Software Assurance personnel.
6. How does your program verify that a provider's software assurance plan meets contractual requirements?
7. Are there current Software Assurance Plans for all applicable (as per SA Classification) Center Projects?
8. Are Software Assurance personnel monitoring changes to operational software?

PROJECT MANAGEMENT:

1. How does your program/project verify that a provider's software assurance plan meets contractual requirements and is followed throughout the project?
2. What audits are conducted on the software project prior to delivery, both by the contractor and by NASA software assurance?
3. What software quality metrics are collected for your software project? Demonstrate how they have been captured and used.

NASA Office of Safety and Mission Assurance
300 E Street SW
Washington, DC 20024-3210
www.hq.nasa.gov

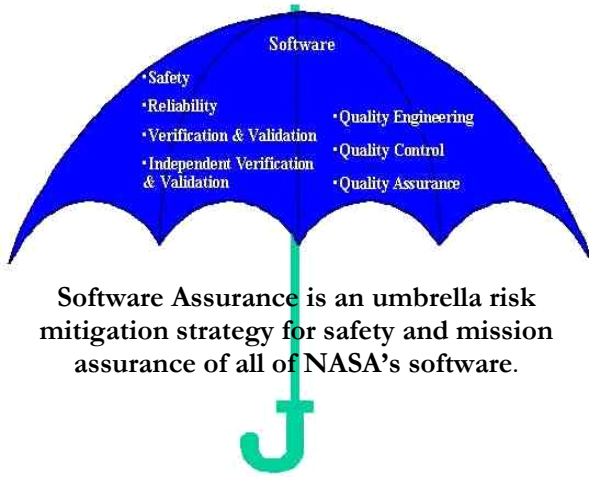
Publication Date August 29, 2005

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
SAFETY AND MISSION ASSURANCE REQUIREMENTS

NASA-STD-8739.8

Software Assurance Standard

Compliance Verification Guide



Software Assurance is an umbrella risk mitigation strategy for safety and mission assurance of all of NASA's software.

http://www.hq.nasa.gov/office/codeq/software/index.htm

OFFICE OF SAFETY AND MISSION ASSURANCE

This brochure is intended to be used as a guide only, not as a replacement for the actual policy. To review Software Assurance Standards (NASA-STD-8739.8) in its entirety, see http://www.hq.nasa.gov/office/codeq/doctree/texttree.htm

Explore. Discover. Understand

Objective of NASA-STD-8739.8

To provide the processes and procedures for analyzing and applying appropriate software assurance techniques and methods to software.

Software Assurance Discipline

- Provides a software life cycle perspective for the minimum required software assurance procedures that contribute to quality software.
- Provides the acquirer and provider requirements for software assurance and software engineering activities to obtain the level of quality, reliability and safety on all software products.
- Provides basic procedures for establishing, operating, and maintaining a software assurance program whether in house or contracted.
- Provides specific requirements for the umbrella process of software assurance and its disciplines of software quality, software reliability, software safety, software verification and validation, and independent verification and validation.

MINIMUM AUDIT POINTS FOR NASA-STD-8739.8

Leadership and Management

- **Acquirer Software Assurance Manager**
  - Shall ensure completion of the Software Assurance Classification Assessment.
    - Objective Quality Evidence (OQE) – System Requirements, Software Assurance (SA) Assessment Reports and Records
  - Shall identify, analyze, track, and control procurement, development and operations SW risks.
    - OQE – SA Reports, Software Risk Analysis, Contract Agreements.
  - Shall verify that software and all related products (e.g. requirements, design, code, documentation and special instructions) are complete and that they meet all of the specified requirements prior to acceptance.
    - OQE – Software Assurance Review and Audit Reports
  - Shall assure that both deliverable and any designated non-deliverable software development products have proper configuration control.
    - OQE – Configuration Control Plans and Records
  - Shall assure that software issues are documented and tracked to resolution.
    - OQE – Problem Resolution Processes
  - Shall assure that software engineering and management prepare, approve, and execute both retirement and operations plans.
    - OQE – Approved Operations & Retirement Plans
- **Provider Software Assurance Manager**
  - Shall obtain software assurance training for management, engineering, and software assurance personnel.
    - OQE – Training Plans and Records
  - Shall flow down the requirements of this Standard to all subcontractors.
    - OQE – Audit Records of Subcontractors

Core Process

- **Acquirer Software Assurance Manager**
  - Shall ensure that software assurance processes are in place for software acquisition, development, maintenance and operation of the software developed or acquired by NASA.
    - OQE – SA Processes and Procedures
- **Provider Software Assurance Manager**
  - Shall plan, document, and implement a software assurance program commensurate with the classes of software identified within the project.
    - OQE – Programs Plans and Procedures
  - Shall assure both acquirer and provider project management are following the software assurance plans and that the quality, reliability and safety of the project's software is properly addressed, raising issues to a higher level if there are concerns not being met by the project.
    - OQE – SA audits, review inputs and reports
  - Shall coordinate with Independent Verification and Validation (IV&V) personnel to share data and information when IV&V has been selected for a project.
    - OQE – IV&V Statements of Work

Process Check

- **Acquirer Software Assurance Manager**
  - Shall ensure that acceptable audits are performed prior to delivery.
    - OQE – Audit Results and Reports
- **Provider Software Assurance Manager**
  - Shall conduct and document periodic reviews, audits, and assessments of the SW development process and products.
    - OQE – Audit reports
- **Acquirer and Provider Software Assurance Engineer**
  - Shall assure that all of the required plans are documented, adhere applicable standards and procedures, are mutually consistent, and are being executed.
    - OQE – Plan Reviews and Reports
  - Shall assure that all software requirements are defined, traceable, from one life cycle phase to another.
    - OQE – Software Requirements Statement
  - Shall assure that software quality metrics are in place and are used to ensure the quality and safety of the software products.
    - OQE – Reports and Analysis
  - Shall assure that formal reviews and inspections are monitored and address software assurance issues.
    - OQE – Monitor Schedule and Reports
- **Acquirer and Provider Software Assurance Engineer and Manager**
  - Shall assure that problems found with the implementation of software life cycle processes are documented, tracked, and resolved.
    - OQE – Problem Resolution Processes and Reports